3.2 Information Technology Policy

3.2.1 Scope

This policy refers to all IT equipment and all users. All users must be given a unique account name and secure confidential password before accessing the Company network. Failure to follow this policy will result in disciplinary action.

3.2.2 Policy

Users must ensure that they comply with current legislation and use the internet and email facility in an acceptable way, ensuring that they do not create unnecessary business risk to the Company by any misuse

The email/facilities may be used for occasional private purposes provided that such use is reasonable does not interfere with the IT infrastructure, or the individual's work ability, violate any Company policy, or dominate the connection bandwidth.

Unacceptable use is classified as:

- Visiting internet sites that contain obscene, racist, offensive pornographic, or other illegal material.
- Using the computer to perpetrate any form of fraud or software, film or music piracy.
- Using the internet to send offensive or harassing material, or to upset other users.
- Using the Internet to send threatening ,abusive or obscene material
- Downloading commercial software, or any copyrighted materials belonging to third parties, unless this download is covered, or permitted, under a commercial agreement, or other such license.
- Hacking into unauthorised areas.
- Reading or copying private emails.
- Creating or transmitting defamatory material.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of computer virus into the corporate network.
- Contravention of the Computer Misuse Act 1990.
- Contravention of the Obscene Publications Act 1959.
- Contravention of the Data Protection Act 1998
- Using IT facilities for a purpose other than that for which you are properly authorised.

If you suspect a virus, stop work immediately, note the symptoms, stop all associated IT use, report the incident immediately to the administrator, do not switch off the PC or remove the network cable from the PC.

The Company maintains the right to monitor the volume of the internet traffic, together with the internet sites visited. Specific content will not be monitored unless there is a suspicion of improper use.

The company will regularly back up appropriate data and maintain disaster recovery plan

The Company will control software usage and issue status.

The IT Policy will be reviewed for compliance and content at each management review.

Signatory: Greg Bell – Managing director

Signed: